au_to_path()

Be careful with paths passed as a parameter

Sean Barnum, Cigital, Inc. [vita[1]]

2005-10-03

Onderdeel "Original Cigital Coding Rule in XML"

Mime-type: text/xml, omvang: 7152 bytes

Identification Difficulty

Scan

Rule Accuracy

False Positives

Priority

Medium

Attack Categories

- Path spoofing or confusion problem
- Malicious Input

Vulnerability Categories

- Indeterminate File/Path
- TOCTOU - Time of Check, Time of Use

Software Context

- File Path Management

Description

The au_to_path() function takes a pathname as an argument. Care must be exercised when accessing files from passed in pathnames. The *au_to_path(char *path) function is used to format an input path name into a path token. A path token contains access path information (token ID, a byte count of the

1. daisy:35 (Barnum, Sean)

path length, and an absolute path) for an object. au_to_path(path) is vulnerable to unknown malicious changes to the path passed as a parameter.

Application Programming Interfaces

Function Name	Comments
au_to_path()	

Method of Attack

The key issue with respect to TOCTOU vulnerabilities is that programs make assumptions about atomicity of actions. It is assumed that checking the state or identity of a targeted resource followed by an action on that resource is all one action. In reality, there is a period of time between the check and the use that allows either an attacker to intentionally or another interleaved process or thread to unintentionally change the state of the targeted resource and yield unexpected and undesired results An attacker could potentially link the passed in path to a path known by the attacker causing failure of the expected path operations as well as potentially leveraging the returned token to access files that should not be accessible at the attackers level of privilege.

Exception Criteria

If proper checking is performed or user-specified input is not used, this is not a problem.

Solutions

Applicability	Description	Efficacy
Generally applies to au_to_path()	The most basic advice for TOCTOU vulnerabilities is to not perform a check before the use. This does not resolve the underlying issue of the execution of a function on a resource whose state and identity cannot be assured, but it does help to limit the false sense of security given by the check.	Does not resolve the underlying vulnerability but limits the false sense of security given by the check.
When the file being altered is owned by the current user and group.	Set your effective gid and uid to that of the current user and group when executing this statement.	This will prevent an attacker from altering any file they can't already alter.
When user specification of the file to be altered is not necessary.	Do not rely on user-specified input to determine what path to format.	This will reduce exposure but will not eliminate the problem.
Generally applies to au_to_path().	Limit the interleaving of operations on files from multiple processes.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.

Generally applies to au_to_path().	Limit the spread of time (cycles) between the check and use of a resource.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
Generally applies to au_to_path().	Recheck the resource after the use call to verify that the action was taken appropriately.	Checking the path permissions after the operation does not change the fact that the operation may have been exploited but it does allow halting of the application in an error state to help limit further damage.

Examples of Incorrect Code

- Example 1

VERBETER

#include

VERBETER

#include

```
/* check permissions to the path */
if(!access(file, ...){
   /* format path into path token */
   au_to_path(path)
}
else{
  /* permission was denied */
}
```

Source References

- ITS4 Source Code Vulnerability Scanning Tool - http://www.cigital.com/its4/
- Viega, John & McGraw, Gary. Building Secure Software: How to Avoid Security Problems the Right Way. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X, ch 9

Recommended Resources

Resource	Link
M. Bishop and M. Dilger, "Checking for Race Conditions in File Accesses," Technical Report, CSE-95-10, September 1995.	http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/ucd-ecs
M. Bishop and M. Dilger, "Checking for Race Conditions in File Accesses," Computing Systems 9 (2) pp. 131-152 (Spring 1996).	http://nob.cs.ucdavis.edu/~bishop/papers/1996-racecond/1996-ra
Solaris 10 Reference Manual Collection	http://docs.sun.com/app/docs/doc/816-5172/6mbb7btaj?q=kstat_read&a=view[5]

5. http://docs.sun.com/app/docs/doc/816-5172/6mbb7btaj?q=kstat_read&a=view

Discriminant Set

Operating Systems

- UNIX

Languages

- C
- C++

Cigital, Inc. Copyright

Velden

Naam	Waarde
Copyright Holder	Cigital, Inc.

Velden

Naam	Waarde
Attack Categories	Malicious Input Path Spoofing or Confusion
Operating System	UNIX
Software Context	File Path Management
Vulnerability Categories	Indeterminate File/Path Time-of-Check/Time-of-Use

1. mailto:copyright@cigital.com